Security Essentials for Fermilab Administrators

Jason Ormes – Fermilab Computer Security

Computer Security Awareness Day

7 December 2016

Outline

- Why Computer Security ?
- Fermilab Strategy:
  - Integrated Computer Security
  - Defense in Depth
  - Central Authentication
  - Central Management
  - Email
  - Reporting computer security incidents
- Your role and responsibilities
  - Web Surfing
  - Activities to avoid
  - Prohibited activities
  - Incidental use
  - Privacy
  - Licensing
  - Tissue & more…

Intro - Why Computer Security ?

- The Internet is a dangerous place
  - We are constantly being scanned for weak or vulnerable systems; new unpatched systems will be exploited within minutes.
- Fermilab is an attractive target
  - Various resources
    - Networks and computers
    - High network bandwidth is useful for attackers who take over lab computers
  - Publicity value of compromising a .gov site
  - Attackers may not realize we have no classified information

Protecting Lab Resources and Reputation

- We need to protect
  - Our data
  - Our ability to use our computers (denial of service attacks)
  - Our reputation with DOE, Congress and the general public
- Major sources of danger
  - Unpatched OS or software – unmanaged system
  - Unaware of services running on system
    - Not turning off unwanted services
  - Running malicious code on your machine due to system or application vulnerabilities or improper user actions
  - Carrying infected machines (laptops) in from off site
  - Falling for Spam and Phishing attempts

FNAL Strategy - Integrated Security Management

- Computer Security is part and parcel of everything you do with computers (analogy with ES&H)
- Not one solution, but appropriate for the needs and vulnerabilities of each system – covered in subsequent slides
- In most cases, knowledge and care are all that is needed to work safely on your computer

FNAL Strategy - Perimeter Controls

- Certain protocols are blocked at the site border
  - email to anything other than lab mail servers
  - web to any but registered web servers
  - other frequently exploited services
- Fermilab Firewall in the near future
  - Replacing the outdated autoblocker

FNAL Strategy - Central Authentication

- Use of lab computing services requires central authentication
- Avoid disclosure of passwords on the network
- Network logon services available on the internet can only be offered by requiring central authentication
  - Kerberos – Login (pw not transmitted over the wire)
    - Windows, OSX & Unix
  - Services – Login (accepted risk – non Kerberos)
    - Email, Service Now, Kronos…
- Lab systems are constantly scanned for violations of this policy

FNAL Strategy – Central Management

- Baseline configurations exist for each major operating system (Windows, Linux, OSX)
- All fermi owned systems must run central management software including anti-virus
- Keep everything up to date with patches and OS versions - even applications!
- The Service Desk will take care of this for your desktop – only rare exceptions

FNAL Strategy - Email

- Users are on the “front line” of computer security
- Phishing/Spam
  - Number one source of Fermilab user account compromise
- Do not click on links unless you know for sure they are safe
- Do not reply to spam as this only confirms your email address is valid
- Don’t trust who email is from
- Do not configure your Fermilab managed email client for non-lab email
  - Major source of virus infections
  - Use webmail instead

FNAL Strategy - Networking

- All machines must be registered to run on the Fermilab network
- Lab network and FGZ
  - The lab network and FGZ wireless is intended for machines preforming lab business
- Guest network
  - Intended for temporary visitors and non Fermilab work related network devices
  - Personal Devices (should connect to guest network)

FNAL Strategy - Computer Security Incidents

- Incident reporting is mandatory
- X2345 or SD ticket or email to computer_security@fnal.gov
- What to do if suspect an incident: DON'T TOUCH THE MACHINE. DON'T TRY TO CLEAN YOURSELF
- Incidents investigated by Fermi Incident Response (FIR)
- Examples of potential incidents
  - User replied to spam and is now sending spam email via web client
  - OSX setup for network sharing acting as a rogue access point
  - Fermilab website defacement
  - Lost/Stolen computing equipment (laptop)
- Fermilab Incident Response (FIR)

Web Surfing - Incidental Computer Usage

- Fermilab permits some non business use of lab computers
- Be careful where you surf, only visit known reputable sites
- We perform web content filtering, malware and AV inspection
- Illegal and adult content prohibited
- Guidelines are at http://security.fnal.gov/ProperUse.htm

Activities to Avoid

- Large grey area, but certain activities are “over the line” –
  - Illegal
  - Prohibited by Lab or DOE policy
  - Embarrassment to the Laboratory
  - Interfere w/ performance of job
  - Consume excessive resources
- Example: P2P (peer to peer) software like Skype and BitTorrent: not explicitly forbidden but very easy to misuse!

Prohibited Activities

- Running a business
- “Blatant disregard” of computer security
- Unauthorized or malicious actions
  - Damage of data, unauthorized use of accounts, denial of service, etc., are forbidden
- Unethical behavior
  - Same standards as for non-computer activities
- Restricted central services
  - May only be provided by approved service owners
- Security & cracker tools
  - Possession (& use) must be authorized
- See http://security.fnal.gov/policies/cpolicy.html

Copyrighted material

- Against lab policy to install if you do not have a proper license
- Possible sources of illegal Copyright software
  - P2P
  - Bittorrent
  - Personal from home
- Risk to the Fermilab network environment
  - Malware and viruses distributed with it
  - Misuse of network resources
- Takedown notices
  - Risk lab embarrassment
  - Possible legal or disciplinary action against the user

Software installation

- Open a SD ticket to have software installed
- 3rd party software may open ports and services to the Internet unbeknownst to you
- E.g. if you need a PDF editor, have the Lab install one
- E.g. If you want a video editor installed for editing home videos, do it at home. Many free software offerings also contain unwanted programs, toolbars, etc
- Installing software
  - If you must do it yourself, READ all the screens. Often times, you need to check or uncheck box to NOT install additional unwanted items such as toolbars, AV engines, etc
  - Ensure it is properly licensed

Local Administrator access

- **NOT granted by default**
- ***NOT*** acceptable to be logged in with local administrator rights as your normal way of working
- Open a Service Desk ticket asking for local administrator access
  - Requirement to provide business case need
  - Access may be removed once you complete administrator work or an agreed upon time
- Laptop users will be given a local account with administrator access for emergencies.
- Try not to log in with –admin credentials unless absolutely necessary. Elevate privileges instead.

Using –admin and –mgr credentials

- Special domain accounts for privileged domain access
- Do not log in directly with –admin or –mgr credentials
  - Use “run as”
  - In some cases 2 factor authentication may be required
  - In some cases a terminal server is required

Securing your computer - Passwords

- Different types of passwords in use
  - Kerberos (Windows login or <username>@FNAL.GOV
  - Services (Kronos FTL, ServiceNow, Exchange email)
- Password care and non-reuse
    - Do not write them down and keep as reminders at your workstation
    - Do not use the same password for different accounts
      - FNAL.GOV or Fermi account different than Services account
- Using a password keeper (KeePass, etc)
  - Many products out there. None officially supported by Fermilab
  - KeePass has worked for CST

Securing your computer - Physical

- Locking the screen
  - Always lock your screen when away from the computer
- Physical locks
  - Machines in unlocked or common areas should use a cable lock to prevent theft

Fermilab VPN Usage

- All computers running on Fermilab VPN and bound to Fermilab Computing Policy
  - This includes personally owned machines
  - May be subject to FIR instructions during an incident
- Ensure you are running a firewall and AV on your home machine before connecting
- Don't leave the VPN session running if others are using the computer
- Only VPN when needed, and disconnect when done

Tissue notices

- TIssue is primarily used for tracking compliance with Computing Security policies.
- It is tightly coupled with both the Fbi (Fermi Blocking Implementation) Ncis (Network Common InfraStructure) and applications
- Virus notice, ssh passwords, webservers, EOL OS, bypassing FNAL security controls
- Can remediate yourself if problem fixed
- Not OK to remediate without fixing the issue. May be re-detected and blocked
- In some cases CST needs to approve the unblock

Bypassing security controls

- Public/private VPN to bypass the Fermilab web proxy
- Disabling AV software on lab managed desktops
- Manually changing the hardware address of your network adapter to bypass a network block
- Any machine bypassing Fermilab security controls will be blocked with the Fermi Blocking Interface (FBI)
    - CST approval for unblock required

Exemptions

- For various reasons you may need to ask for an exemption from Lab policy to perform your work related obligations.
- Types of exemption requests via ServiceNow
  - Scanner Farm exemption
  - End of Life Operating System
  - Web Directory Exemption Request
- You will be required to provide details of the request and your alternate means of securing your machine.
- In some cases you may be asked to present your request to the CSBoard.
- In general renewable every year - possibly shorter.

Backing up files

- You are responsible for backing up your data files
- Be sure to know where to place files for backups (e.g. file servers)
- Cloud file storage
  - Use only for non-Lab business (Lab may need to retrieve files in the event you leave)
  - Use Lab approved cloud storage (currently OneDrive) for Lab business

Privacy

- Fermilab normally respects the privacy of electronic files and email
- Employees and users are required to do likewise
- If access to other users files is needed, it *must* have Director(ate) approval
  - Certain exemptions for Fermilab Incident Response
  - Certain exemptions for supervisors of employees no longer at the lab
- Cannot browse user files without consent
- Report illegal activities
- Sniffing allowed only on the machine you are troubleshooting, and only for the duration of troubleshooting

Antivirus

- Antivirus enabled on centrally managed Windows or OSX machines
- Non centrally managed or personal?
  - Run it, even on Mac
- Linux: run it if offering Windows shares

Mandatory System Manager Registration

- System managers must be registered with MISCOMP SysadminDB
  - System managers are - the person(s) responsible for configuring, maintaining and supporting a system and installing patches
  - Automatically subscribed to cppm-reg-sysadmins@fnal.gov mail list
- Go to http://security.fnal.gov and click on “verify your node registration” to see who is registered as sysadmin for your system

Critical Vulnerabilities and Vulnerability Scanning

- Certain security vulnerabilities are declared critical when they are (or are about to) being actively exploited and represent a clear and present danger
- Systems must be patched by a given date or they will be blocked from network access
- This network block remains until remediation of the vulnerability is reported to the TISSUE
- Notifications are sent to registered System Administrators
- http://security.fnal.gov for the latest list of critical vulnerabilities

Firewalls

- Know what is running on the machines you support to the best extent possible
- Firewalls enabled on centrally managed machines
- Should be enabled on non centrally managed machines
- Only run necessary services
  - Default deny
  - Open ports as needed
- Only open services to the subnets you intend access from
- May be blocked if certain services are exposed off site
- Fermilab network is being monitored for exposed ports and services

Remote Access

- Use Bomgar when possible
- RDP is permitted from FNAL only using domain credentials
- VNC and others must be inside a Kerberized session such as Kerberized SSH
- Vendor and visitor screen sharing can only be used if the user is present at the machine, watching their actions

Risk assessments

- If you are setting up a new application or technology, you must write a risk assessment to document risks and appropriate controls.
- If you are adding new features to an existing (and approved) risk assessment, it must be revised.
- These will be reviewed by CSBoard. There may be a possibility it may not be approved if the risks prove to be too great.

Major/minor applications

- Defined as “critical to the mission of the Laboratory”, i.e. additional risks and disruption may have major impact on Laboratory operations
  - Most things do *not* fall in this category (business systems, AV server, central management servers)
- Special (more stringent) rules & procedures apply; each MA has its own security plan with enhanced and compensatory security controls beyond the baseline security controls
- You’ll know if you’re in this category

Computing Policies

- Read Fermilab Policy on Computing
  - http://cd-docdb.fnal.gov/cgi-bin/RetrieveFile?docid=1186

- Assorted Computing Policies at Fermilab
  - http://computing.fnal.gov--> Computing Policies link
    - https://fermipoint.fnal.gov/organization/cs/SitePages/Computing%20Policies.aspx

Questions?

- x2345 24x7 for reporting urgent security incidents

- Service Desk ticket for questions about security policy
- http://servicedesk.fnal.gov

- computer_security@fnal.gov for reporting non-urgent security incidents
- http://security.fnal.gov/

Training Requirement complete

- Security Essentials for Fermilab System Administrators
  - [FN000370/CR/01]

Thank you for attending!